National SCADA Test Bed

Fact Sheet

Benefits

Working in partnership with the energy sector, the National SCADA Test Bed seeks to

- Identify and mitigate existing vulnerabilities.
- Facilitate development of security standards.
- Serve as an independent entity to test SCADA systems and related control system technologies.
- Identify and promote best cyber security practices.
- Increase awareness of control systems security within the energy sector.
- Develop advanced control system architectures and technologies that are more secure and robust.

Purpose

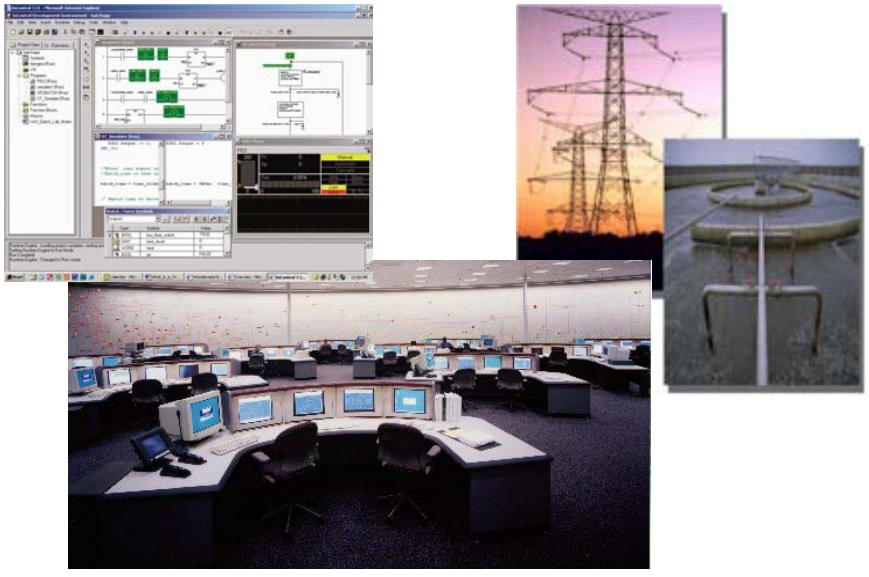
The NSTB supports industry and government efforts to enhance the cyber security of control systems used throughout the electricity, oil, and gas industries.

PROTECTING ENERGY SYSTEMS BY IMPROVING THE SECURITY OF CONTROL SYSTEMS

Improving the security of energy control systems has become a national priority. Since the mid-1990's, security experts have become increasingly concerned about the threat of malicious cyber attacks on the vital supervisory control and data acquisition (SCADA) systems used to monitor and manage the flow of electricity and fuels through our critical energy infrastructure. Most SCADA system designs did not anticipate the security threats posed by today's reliance on common software and operating systems, public telecommunication networks, and the Internet. The 2003 *National Strategy to Secure Cyberspace* urged government and industry to develop new technologies and best practices to address these vulnerabilities and strengthen the security of these systems. Until recently, however, energy systems owners and operators found it difficult to assess the vulnerability of their operational control systems and to test and verify the performance of proposed security upgrades prior to installation.

The National SCADA Test Bed (NSTB) applies a national testing environment to help secure SCADA communications and controls within the energy sector. It combines the expertise and resources of several national laboratories into a multi-lab partnership that helps to identify and correct critical security flaws in SCADA equipment and control systems.

The DOE Office of Electricity Delivery and Energy Reliability (OE) seeks to improve the security and reliability of our Nation's energy delivery systems. OE established the NSTB to help the energy sector and equipment vendors assess control system vulnerabilities and test the security of control systems hardware and software. The test bed employs a full-scale infrastructure suite of facilities for testing and validating control systems. Jointly run by Sandia National Laboratories and the Idaho National Laboratory, the NSTB offers the integrated expertise and resources of multiple national laboratories, including Argonne National Laboratory (oil and gas infrastructure), Pacific Northwest National Laboratory (electricity infrastructure), and the National Infrastructure Simulation and Analysis Center.



Partners

Idaho National Laboratory

Sandia National Laboratories

Argonne National Laboratory

Pacific Northwest National Laboratory

National Institute of Standards and Technology

For more information about the National SCADA Test Bed, contact:

Robert Hill
Project Manager, NSTB
Idaho National Laboratory
P.O. Box 1625
Idaho Falls, ID 83415-2604
208-526-8306
robert.hill@inl.gov

Tommy Cabe
Sandia Project Lead, NSTB
Sandia National Laboratories
P.O. Box 5800/MS 1368
Albuquerque, NM 87185-1368
505-845-8032
tjcabe@sandia.gov

For Program Information, Contact:

Hank Kenchington
Program Manager
U.S. Department Energy
Office of Electricity Delivery and Energy Reliability
1000 Independence Ave., SW
Washington D.C. 20585
202-586-1878
henry.kenchington@hq.doe.gov

A National Resource for Industry

The NSTB is a national resource for identifying and solving today's SCADA vulnerability issues, testing new and existing equipment, and developing next-generation architectures and technologies. Primary goals are to accomplish the following:

- Raise industry awareness of system vulnerability issues and mitigation techniques.
- Collaborate with industry to identify, assess, and mitigate current SCADA system vulnerabilities.
- Work with industry to develop near-term solutions and risk mitigation strategies for existing systems.
- Develop long-term best practices as well as next-generation architectures for intelligent, inherently secure and dependable control systems and infrastructures.
- Support development of national standards and guidelines for more secure control systems.

The NSTB leverages the extensive, expert capabilities of the participating national laboratories to support the development of a more secure and reliable energy infrastructure. The NSTB provides modeling and simulation resources; comprehensive technical expertise in industrial SCADA systems; facilities that recreate real-world control systems, infrastructures, and networks; red team and assessment expertise; cryptography and information security capability; research and guidance for standards development; and other SCADA-related test bed and security activities.

Facility Resources

The NSTB draws on a network of assets and capabilities available at the Critical Infrastructure Test Range (INL) , the Center for SCADA Security (SNL), and participating laboratories. Assets and capabilities include the following:

- Next Generation Wireless Test Bed (3G/4G testing; local area network and 802.11 testing)
- Power Grid Test Bed (61 miles of 138 kV transmission loop; 7 substations)
- Cyber Security Test Bed (vulnerability assessments; intrusion detection expertise)
- SCADA Security Training Courses (Best Practice Course; Assessment Course)
- Virtual SCADA Environment
- Specialized laboratories for Cryptography, Network Security, and Intelligent Infrastructure R&D

Progress and Milestones

Since 2003, the NSTB has assessed the vulnerability of three major SCADA systems and recommended security enhancements to the vendors. The vendors have adopted those recommendations, developed next generation systems and worked with end-users to implement upgrades in legacy systems.

NSTB publications:

- *ABB SCADA/EMS System, INEEL Baseline Summary Test Report*
- *A Summary of Control System Security Standards Activities in the Energy Sector*
- *Network Security Infrastructure Testing*
- *Reference Model for Control and Automation Systems in Electrical Power*

Current NSTB activities:

- Assessment of SCADA/Systems
- Development of self-assessment methods
- Analysis of common IT anti-virus applications for control systems
- Functional and cryptographic testing of a simulated AGA 12-1 implementation
- Security standards gap analysis
- Development of a Virtual SCADA Environment modeling tool
- Analysis and testing of proposed Secure ICCP protocol
- Conduct of Control System security workshops